UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/072,260	02/06/2002	James D. Pravetz	07844-497001	3277

21876 7590 08/04/2008

FISH & RICHARDSON P.C.
P.O. Box 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
BROWN, CHRISTOPHER J	
ART UNIT	PAPER NUMBER
2134	
MAIL DATE	DELIVERY MODE
08/04/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/072,260	PRAVETZ, JAMES D.	
	Examiner	Art Unit	
	CHRISTOPHER J. BROWN	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 March 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,11-14,16-31 and 33-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9, 11-14, 16-20, 23, 24, 16-31, 33-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *5/1/08*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

.

Response to Arguments

Applicant's arguments, with respect to the rejection(s) of independent claim(s) under USC 101, 112, and 103 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Pashupathy US 6,078,951.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-7, 9-10, 12-14, 16, 17, 19, 23, 24, 26-28, 30, 31, 33-36, 38-39, 41-46, 48, and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jilk, Jr. US 2002/0010746 in view of Dusse et al RFC 2311 in view of Pashupathy US 6,078,951

RFC 2312 and 2311 are used herein as definitions of the S/MIME message format. RFC 2311 has been referred to as Dusse without further indication while RFC 2312 has been referred to as 2312 since the authors of both RFCs are the same.

Jilk teaches a system for requesting web pages through a forms format over electronic mail, wherein containers are generated and sent between applications, but fails to explicitly teach certificate exchange for secure communications of these web pages.

However, in related art, Dusse teaches a system for secure container type attachments (S/MIME), wherein certificates are automatically exchanged between parties for purposes of secure communications. It is an advantageous feature within web communications to be able to provide for secure communications of content wherein the nature of the content is not limited by sensitivity of the material being communicated since protection is afforded by cryptographic techniques (Dusse pg 1 lines 8-25; Jilk paragraphs 12-16).

Pashupathy teaches a plugin application to allow an application regarding MIME containers to be used in conjunction with a web browser email program.

It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the systems of Jilk, Dusse, and Pashupathy to allow for reception of all web content including such content that is typically secure by implementing the secure communication.

Regarding Claim 1: First application on a client to generate a first container object with a recognizable container type which is associated with the first application (Jilk paragraphs 17-18, 21, 23, 97; 2312 section 2.2, 2.3) The process of utilizing S/MIME dictates that certificates are exchanged prior to communication in order to provide for the secured communications. This

process clearly creating a container with a plugin (1st application), which contains the sender's certificate and a request for a recipient's certificate. The 2nd application in this case is considered to be an email program.

Containing a sender's certificate or request for a recipient's (Dusse pg 21 lines 28-38, pg 22 lines 1-2; 2312 section 2.3; Jilk Figs 3b, 10, 12, paragraphs 97)

Generating the first container object includes putting the certificate or request in the container object (2312 section 2.3) Clearly section 2.3 outlines including the certificate for the originator (sender) in order to be able to establish the trusted communications.

Using a second application distinct from the first to transmit the container to a recipient's address (Jilk Figs 3, paragraph 96 lines 9-30, 97) The system of Jilk provides for sending the container via email, the use of email dictates that the email program produces the container (email) and then passes the composed message with the certificates to an OS module such as WinSock which formats the message according to network protocols and sends the message.

obtaining a second container object having the same type as the first from the second application (Jilk Figs 3 paragraph 97) The email application clearly receives any response from WinSock wherein the container object type is of a standard email format.

automatically identify and extract one or more certificates (Dusse sections 2.4.2 – 2.5, 2.6.1, pg 9 section 3 – pg 10 3.1, pg 1, pg 21 line 28 – pg 22 line 2; 2312 section 2.3, pg 6-7 section 4) From the discussion of Dusse, which states that "S/MIME can be used in automated message transfer agents that use crypto security services that do not require human intervention" and that such services as encryption and non-repudiation are provided by S/MIME. The reception of an initial message dictates that a certificate is provided to the client so that the content may be decrypted

or a signature automatically verified which inherently requires extraction of a certificate in order to obtain the associated public key. As described by rfc 2312 a message is provided and signed that contains the certificate and a request for the recipients certificate. This functionality is clearly included within the initial message of the Jilk system as is necessary to facilitate communications.

Pashupathy teaches a first application plugin system for utilizing MIME applications in a web browser. (Col 1 lines 24-31, Col 4 lines 30-60).

It would have been obvious to one of ordinary skill in the art to use the plugin application because it expands the user's options for viewing files with a web browser.

Regarding Claim 2: Receive input from sender specifying recipient's address (Jilk Fig 6, 18, paragraph 96 lines 9-30, 88, 97; 2312 section 3.1) As within any typical email message the system must provide for the destination or recipient with which the communication is desired. Receiving input specifying one or more certificates of the sender (Dusse sections 2.4.2 – 2.5, 2.6.1, pg 9 section 3 – pg 10 3.1, pg 1, pg 21 line 28 – pg 22 line 2; 2312 section 2.3, pg 6-7 section 4) The process of public key encryption wherein the services are used for signing and encrypting dictate that the signing functionality requires a certificate of the sender to be included so that the recipient may authenticate, furthermore, the protocol for S/MIME dictates that upon initial communication a signed certificate is sent in a message. It is therefore an inherent feature wherein more than a single certificate exists on the client for the client to specify which certificate is to be used.

Regarding Claims 3, and 19: transmitting/receiving the container by electronic mail (Jilk paragraphs 23-24, 96 lines 9-30, 97)

Transmitting/receiving by HTTP (Jilk Fig 1, paragraphs 23-24) As stated above the system provides for electronic mail over the internet. As it is known electronic mail is not confined to a single method but is provided for in many ways. Electronic mail is available over the internet via web-based email services such as Yahoo.com for example. In such an exemplary situation the container or message is communicated over HTTP to the end user for viewing, as such providing for transmission by HTTP. Furthermore, Jilk provides for request via a web browser, which would then define the container as a request over HTTP.

Transmitted/Received via a networked server (Jilk Fig 1, paragraphs 23-24, 96 lines 9-30, 97) The communications of any standard mail service require submission via a mail server.

Transmitting the recipients certificate back to the sender (Dusse sections 2.4.2 – 2.5, 2.6.1 – 2.6.2.4, pg 9 section 3 – pg 10 3.1, pg 1, pg 21 line 28 – pg 22 line 2; 2312 section 2.3, pg 6-7 section 4) The process of negotiating encryption between the two entities requires knowledge of a recipient's certificate, specifically section rfc 2311 and 2312 sections 2.3 and 4 state that a sending agents should include certificates for the public keys. From those passages it is clear that initial communications mandate the sender providing a certificate and a reply thereto containing the certificate of the recipient (sender of the reply) in order to facilitate secure communications either through signatures or other forms of encryption.

Regarding Claim 4: First container object generated by a server (Jilk Fig 1) In the embodiment discussed in Fig 3b the server initiates the first container.

Regarding Claims 5 and 16: Determine if user has multiple certificates; Receive input selecting one or more of the multiple certificates; Retrieve the selected certificates from a database (Dusse 2312 pg 3-4 section 2.3, pg 6-7 section 4) Clearly selection of the recipients appropriate certificate is inherent when sending a message which is secured wherein more than a single certificate is available. As disclosed in rfc 2312 by discussion of a database for particular recipients and there associated certs.

Include the selected certificates in the container object (Dusse 2312 pg 3-4 section 2.3, pg 6-7 section 4) As noted the certificates are incorporated into the container (message).

Regarding Claim 6: receive input from sender specifying a return address (Jilk Fig 3b, 7, 18, paragraphs 97, 116, 121) The functionality of an electronic mail system requires the sender's address to be incorporated into the outgoing message, and in some cases the user may present an alternate reply address as outlined.

Instructions for returning recipient's certificate (Dusse 2312 pg 3-4 section 2.3, pg 6-7 section 4) The instructions for returning the certificate are simply the request itself and the return address as provided.

Include address and instructions in the first container object (Dusse pg 21 line 28 – pg 22 line 2, 2312 pg 3-4 section 2.3, pg 6-7 section 4) The implementation of S/MIME dictates that a return of a certificate occurs in a first message from that entity.

Regarding Claims 7, 17, and 22: object validation information to be used to validate the certificate (Dusse sections 2.4.2-2.5, pg 21 line 28 – pg 22 line 2; 2312 pg 3-4 section 2.3, pg 6-7 section 4, section 4.2 pgs 7-8) This is provided generally by way of singing the

certificate/message with the private key of the sending party and authenticating that with the public key, which is included with the certificate.

Regarding Claim 9: automatically receive a container from the second application having a recognizable MIME type (Jilk Figs 3b, 7a, 18, paragraphs 23-24, 87-88, 91, 96 lines 9-30, 97, 100-102) The reference provides for receiving email content via an a plugin application which receives those via email (2nd) application.

MIME container type; automatically obtaining the container from the first application (Jilk Fig 7a, 9, 18, paragraph 23, 121; Dusse pg 1) As stated previously the email app automatically receives incoming emails from the winsock client.

Recognize the container may include a certificate; Automatically determine if the container object contains a certificate of the sender (Dusse sections 2.4.2-2.5, pg 21 line 28 – pg 22 line 2; 2312 pg 3-4 section 2.3, pg 6-7 section 4, section 4.2 pgs 7-8) The process of validating the sender inherently provides for making the determination of the presence of a certificate so as to provide for verifying the signature or decrypting the message.

Regarding Claim 12: If certificate is valid, extract and store certificate (Dusse 2312 pg 3-4 section 2.3, pg 6-7 section 4, section 4.2 pgs 7-8) The certificate if validated allows for reading of the message and decryption of the encrypted content and thus it is stored within the memory of the system. In the event a message does not authenticate it would not be retained since an invalid message serves no purpose but to waste resources of the system. Additionally, as discussed by Dusse a database is supplied with the listing of certificates for known entities, thus a recipient clearly stores valid certificates.

Regarding Claims 13, 50: Automatically determine if the first container object has a request for a recipient's certificate (Dusse 2312 pg 3-4 section 2.3, pg 6-7 section 4, section 4.2 pgs 7-8) The certificate exchange outline denotes that the first message containing the sender's certificate is essentially a request for the recipient's certificate.

Regarding Claim 14: Generate a second container including a certificate of the recipient; Extract a return address from the first container and transmit second container to that address (Jilk Fig 3-4, 7a, 9, 18, paragraph 23-24, 96-98, 121; Dusse 2312 pg 3-4 section 2.3, pg 6-7 section 4, section 4.2 pgs 7-8) As noted the certificate is included in a reply to the sender's request; The structure of the message as outlined previously provides for a return address. A second container is generated in accordance with an additional request of the initial container for a new page or service.

Claims 23, 24, 26-28, 30, 31, 33-36, 38-39, 41-46, 48 are a computer program product instruction and method implementation of claims 1-7, 9, 12-17, 19, and as such are rejected on the same basis.

Claims 8, 11, 18, 20, 29, 37, 40, 47, 49, and 51 as best understood are rejected under 35 U.S.C. 103(a) as being unpatentable over Jilk, Dusse and Pashupathy as applied to claim 1, and further in view of The PDF Reference, Second Edition.

Jilk, Dusse and Pashupathy teach a system as in claim 1 for the exchange of certificates via electronic mail via secure communications of web pages that contain forms, but fail to teach the use of Forms Data Format.

The PDF Reference, Second Edition teaches the use of The Forms Data Format for submission and retrieval of information (pg 485 lines 1-26) via a server.

Separating out extra information from a message and forming it into a common file layout is a desirable feature since this process adds cross-platform compatibility and the advantages of increased security by allowing further methods of protecting the given data and additionally adding further functionality through the ability to append such a file to any message format.

It would have been obvious to one skilled in the art at the time of the applicant's invention to combine the Forms Data Format of the PDF Reference, Second Edition with the system outlined by Jilk, Dusse and Pashupathy. The added functionality and security features that are obtained from such a combination being desirable advantages within such a communications system.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER J. BROWN whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571)272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christopher J Brown/ 7/3/08
Primary Examiner, Art Unit 2134